

# Standards Proposal Ballot+Clean

TIA/EIA SP-3580+Clean

\*\*First Post Ballot Version—Subject to Change\*\*

Jul 15, 1997

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

File: Cover.FRM last modified at July 15, 1997 7:10 PM

**TR-45**

# ***Lawfully Authorized Electronic Surveillance***

***TIA/EIA  
SP  
3580+Clean  
al***

©Copyright Telecommunications Industry Association 1997

All rights reserved.

This document is subject to change.

## Abstract

---

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a “safe harbor” under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: “a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106.”

## Document Revision History

Date	Reason for Change
	Initial revision approved for publication.

# Contents

Abstract .....	i
Document Revision History .....	ii
Contents .....	iii
List of Tables .....	viii
List of Figures .....	ix
Foreword .....	xi
1 Introduction .....	1
1.1 General .....	1
1.2 Purpose .....	2
1.3 Scope .....	2
1.4 Organization .....	2
2 References .....	3
3 Definitions and Acronyms .....	4
4 Stage 1 Description: User Perspective .....	13
4.1 Overview .....	13
4.2 Introduction .....	13
4.2.1 Assumptions .....	13
4.2.2 General Background .....	14
4.2.3 Call Content Channels and Call Data Channels .....	15
4.3 Non-Call Associated Information Surveillance Service Description—Serving System IAP 17	
4.4 Call Associated Information Surveillance Service Description—Call-Identifying Information IAP 17	
4.5 Content Surveillance Service Description .....	18
4.5.1 Circuit IAP .....	19
4.5.2 Packet Data IAP .....	22
4.6 Restrictions .....	26
4.6.1 Lack of CDC and CCC Synchronization .....	26
4.6.2 CDC Congestion .....	26
4.6.3 CCC Exhaustion .....	26
4.6.4 CCC Congestion .....	26
5 Stage 2 Description: Network Perspective .....	27
5.1 Introduction .....	27
5.2 Stage 2 Methodology .....	27
5.3 Network Reference Model .....	28
5.3.1 Functional Entities .....	28
5.3.1.1 Access Function (AF) .....	28
5.3.1.2 Delivery Function (DF) .....	29
5.3.1.3 Collection Function (CF) .....	29
5.3.1.4 Service Provider Administration Function (SPAF) .....	30
5.3.1.5 Law Enforcement Administration Function (LEAF) .....	30
5.3.2 Interface Reference Points .....	30

5.3.2.1	Reference Point a .....	30	1
5.3.2.2	Reference Point b .....	30	2
5.3.2.3	Reference Point c .....	30	3
5.3.2.4	Reference Point d .....	30	4
5.3.2.5	Reference Point e .....	31	5
5.4	Message Descriptions .....	31	6
5.4.1	Answer .....	32	7
5.4.2	CCClose .....	33	8
5.4.3	CCOpen .....	34	9
5.4.4	Change .....	35	10
5.4.5	Origination .....	35	11
5.4.6	PacketEnvelope .....	37	12
5.4.7	Redirection .....	38	13
5.4.8	Release .....	39	14
5.4.9	ServingSystem .....	40	15
5.4.10	TerminationAttempt .....	41	16
6	Stage 3 Description: Implementation Perspective .....	42	17
6.1	Protocol Definition .....	42	18
6.2	CDC Protocol Definition .....	4	19
6.2.1	CDC Underlying Data Transmission .....	42	20
6.2.2	CDC Parameter Encoding Objectives .....	42	21
6.2.3	CDC Syntax Definitions .....	43	22
6.3	CDC Message Definitions .....	44	23
6.3.1	Answer Message .....	44	24
6.3.2	CCClose Message .....	45	25
6.3.3	CCOpen Message .....	45	26
6.3.4	Change Message .....	45	27
6.3.5	Origination Message .....	46	28
6.3.6	PacketEnvelope Message .....	47	29
6.3.7	Redirection Message .....	48	30
6.3.8	Release Message .....	48	31
6.3.9	ServingSystem Message .....	49	32
6.3.10	TerminationAttempt Message .....	49	33
6.4	CDC Parameter Definitions .....	49	34
6.4.1	BearerCapability .....	49	35
6.4.2	CallIdentity .....	50	36
6.4.3	CaseIdentity .....	50	37
6.4.4	CCCIIdentity .....	50	38
6.4.5	IAPSystemIdentity .....	51	39
6.4.6	Location .....	51	40
6.4.7	PartyIdentity .....	51	41
6.4.8	PDUType .....	52	42
6.4.9	RedirectedFromInformation .....	52	43
6.4.10	TimeStamp .....	53	44
6.4.11	TransitCarrierIdentity .....	53	45
6.5	CCC Protocols .....	54	46
6.5.1	CCC Encoding for Circuit-Mode Services .....	54	47
6.5.2	CCC Encoding for Packet-Mode Services .....	54	48
6.6	LAESP Compatibility Guidelines .....	54	49
6.6.1	Guidelines For Forward Compatibility .....	54	50
6.6.2	Guidelines For Backward Compatibility .....	55	51
6.6.2.1	Existing Messages .....	55	52

6.6.2.2	Parameters in Existing Messages .....	55
6.6.2.3	New Messages .....	56
6.6.2.4	New Parameters .....	56
6.6.2.5	New Parameter Fields .....	56
6.6.2.6	New Parameter Values .....	56
<b>Annex A</b>	<b>Deployment Examples .....</b>	<b>57</b>
A.1	Possible Network Deployment of IAPs .....	57
A.2	Access and Delivery Function Equipment Configuration .....	58
A.3	Implementation of the d-interface .....	62
A.4	Implementation of the e-interface .....	64
A.5	Possible CDC Protocol Stacks .....	66
A.6	Possible CCC Protocol Stacks .....	67
<b>Annex B</b>	<b>CCCC Delivery Methods .....</b>	<b>70</b>
B.1	Overview .....	70
B.2	Dedicated Circuit CCC Delivery .....	72
B.2.1	Obtain Network Address of Destination .....	73
B.2.2	Setup CCC to Destination .....	73
B.2.3	Destination Acceptance or Refusal of a CCC .....	73
B.2.4	CCC Continuity Verification .....	74
B.2.5	Associate Intercept Subject and Call Identity to the CCC .....	74
B.2.6	Call Content Transfer .....	74
B.2.7	Early CCC Release by the Destination .....	74
B.2.8	Disassociate CCC .....	75
B.2.9	Normal CCC Release by the Source. ....	75
B.3	Trunk Group CCC Delivery .....	76
B.3.1	Obtain Network Address of Destination .....	77
B.3.2	Setup CCC to Destination .....	77
B.3.3	Destination Acceptance or Refusal of a CCC .....	78
B.3.4	CCC Continuity Verification .....	81
B.3.5	Associate Intercept Subject and Call Identity to the CCC .....	81
B.3.6	Call Content Transfer .....	82
B.3.7	Early CCC Release by the Destination .....	82
B.3.8	Disassociate CCC .....	83
B.3.9	Normal CCC Release by the Source .....	83
B.4	Static Directory Number CCC Delivery .....	84
B.4.1	Obtain Network Address of Destination .....	85
B.4.2	Setup CCC to Destination .....	85
B.4.3	Destination Acceptance or Refusal of a CCC .....	85
B.4.4	CCC Continuity Verification .....	86
B.4.5	Associate Intercept Subject and Call Identity to the CCC .....	86
B.4.6	Call Content Transfer .....	86
B.4.7	Early CCC Release by the Destination. ....	86
B.4.8	Disassociate CCC .....	87
B.4.9	Normal CCC Release by the Source .....	87
B.5	Packet Data CCC Delivery .....	87
B.5.1	Obtain Network Address of Destination .....	88
B.5.2	Setup CCC to Destination .....	88
B.5.3	Destination Acceptance or Refusal of a CCC .....	88
B.5.4	CCC Continuity Verification .....	88
B.5.5	Associate Intercept Subject and Call Identity to the CCC .....	89
B.5.6	Call Content Transfer .....	89



B.5.7	Early CCC Release by the Destination .....	89	1
B.5.8	Disassociate CCC .....	89	2
B.5.9	Normal CCC Release by the Source .....	89	3
B.6	Delivery Bearer Service .....	89	4
B.7	Separated Content Delivery .....	90	5
B.8	Combined Content Delivery .....	90	6
B.9	Delivery of Signaling for the Intercepted Call .....	91	7
B.10	Call Content Delivery Delay .....	91	8
B.11	Call Content Distribution .....	92	9
B.12	DTMF C-Tone Signaling Procedures .....	92	10
Annex C	CCDC Delivery Methods .....	94	11
C.1	Dedicated Data Circuit CDC Delivery .....	94	12
C.2	Dedicated Data Link CDC Delivery .....	95	13
C.3	Call Data Distribution .....	95	14
Annex D	Information Access Scenarios .....	96	15
D.1	Simple Abandoned Call Attempt .....	100	16
D.2	Partial Dial Abandon .....	100	17
D.3	Pre-Answer Abandon .....	101	18
D.4	Simple Outgoing Call .....	102	19
D.5	Re-Origination .....	103	20
D.6	Simple Incoming Call .....	104	21
D.7	Call Waiting and Recall .....	105	22
D.8	Call Waiting with Talking Party Disconnect .....	107	23
D.9	Call Held and Retrieved .....	108	24
D.10	Three-Way Calling, Plus Call Turned Away .....	108	25
D.11	Call Forwarding—No Answer on a Single System .....	111	26
D.12	Call Forwarding—No Answer on Different Systems .....	112	27
D.13	Two Bearer Channels, Plus Call Transfer .....	113	28
D.14	Outgoing Call, Plus Three-Way Calling .....	114	29
D.15	Speed Calling .....	115	30
D.16	Multiple Translations on Single System .....	116	31
D.17	Multiple Call Scenario .....	117	32
D.18	Simple Call Delivery to a Mobile Station .....	118	33
D.19	Password Call Acceptance and Flexible Alerting .....	120	34
D.20	Password Call Acceptance and Call Forwarding .....	121	35
D.21	Completed Call To Busy Subscriber .....	122	36
D.22	Dialed Feature Code Digits .....	122	37
D.23	Call Release to Pivot .....	124	38
D.24	Intrasystem Handoff .....	125	39
D.25	Handoff to a Third System without Path Minimization .....	126	40
D.26	In-Call Modification .....	128	41
D.27	Connected Party Modification .....	128	42
Annex E	Optional Messages .....	129	43
E.1	ConnectionTest Message .....	129	44
Index	.....	131	45

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## List of Tables

<i>Table 1:</i>	Answer Message Parameters	32
<i>Table 2:</i>	CCClose Message Parameters	33
<i>Table 3:</i>	CCOpen Message Parameters	34
<i>Table 4:</i>	Change Message Parameters	35
<i>Table 5:</i>	Origination Message Parameters	36
<i>Table 6:</i>	PacketEnvelope Message Parameters	37
<i>Table 7:</i>	Redirection Message Parameters	38
<i>Table 8:</i>	Release Message Parameters	39
<i>Table 9:</i>	ServingSystem Message Parameters	40
<i>Table 10:</i>	TerminationAttempt Message Parameters	41
<i>Table 11:</i>	IAP Primary Locations	57
<i>Table 12:</i>	Simple Switch Connections	97
<i>Table 13:</i>	Simple Abandoned Call Attempt Scenario	100
<i>Table 14:</i>	Partial Dial Abandon Scenario	100
<i>Table 15:</i>	Pre-Answer Abandon Scenario	101
<i>Table 16:</i>	Simple Outgoing Call Scenario	102
<i>Table 17:</i>	Alternate Steps for en bloc Sending	102
<i>Table 18:</i>	Re-origination Call Scenario	103
<i>Table 19:</i>	Alternate Re-origination Call Scenario Steps	104
<i>Table 20:</i>	Simple Incoming Call Scenario	104
<i>Table 21:</i>	Call Waiting with Recall Scenario	105
<i>Table 22:</i>	Call Waiting with Talking Party Disconnect Scenario	107
<i>Table 23:</i>	Call Held and Retrieved Scenario	108
<i>Table 24:</i>	Three-Way Calling, Plus Call Turned Away Scenario	109
<i>Table 25:</i>	Call Forwarding—No Answer on a Single System Scenario	111
<i>Table 26:</i>	Call Forwarding—No Answer on Different Systems Scenario	112
<i>Table 27:</i>	Two Bearer Channels, Plus Call Transfer Scenario	113
<i>Table 28:</i>	Outgoing Call, Plus Three-Way Calling Scenario	114
<i>Table 29:</i>	Speed Calling Scenario	115
<i>Table 30:</i>	Multiple Translations on a Single System Scenario	116
<i>Table 31:</i>	Multiple Call Scenario	117
<i>Table 32:</i>	Simple Call Delivery Scenario	118
<i>Table 33:</i>	Password Call Acceptance and Flexible Alerting Scenario	120
<i>Table 34:</i>	Password Call Acceptance and Call Forwarding Scenario	121
<i>Table 35:</i>	Completed Call To Busy Subscriber	122
<i>Table 36:</i>	Dialed Feature Code Digits Scenario	123
<i>Table 37:</i>	Call Release to Pivot Scenario	124
<i>Table 38:</i>	Intrasystem Handoff Scenario	125
<i>Table 39:</i>	Handoff to a Third System without Path Minimization Scenario	126
<i>Table 40:</i>	In-Call Modification Scenario	128
<i>Table 41:</i>	Connected Party Modification Scenario	128
<i>Table 42:</i>	ConnectionTest Message Parameters	129

## List of Figures

<i>Figure 1:</i>	Electronic Surveillance Model	14
<i>Figure 2:</i>	Call Content Channels and Call Data Channels	16
<i>Figure 3:</i>	Circuit IAP for a Two-Way Communication	19
<i>Figure 4:</i>	Circuit IAP for a Multi-Party Communication	20
<i>Figure 5:</i>	Circuit IAP for an Incoming Call	21
<i>Figure 6:</i>	Circuit IAP for a Redirected Call	22
<i>Figure 7:</i>	Packet Data IAP to a Separated CCC (appropriate to all data services)	23
<i>Figure 8:</i>	Packet Data IAP to a Combined CCC (connectionless data services only)	24
<i>Figure 9:</i>	Packet Data IAP to a CDC (for selected packet types)	25
<i>Figure 10:</i>	Network Reference Model	28
<i>Figure 11:</i>	Land Line IAPs	57
<i>Figure 12:</i>	Mobile Intercept Subject's Home System IAPs	58
<i>Figure 13:</i>	Mobile Intercept Subject's Serving System IAPs	58
<i>Figure 14:</i>	Mobile Intercept Subject's Redirecting System IAPs	59
<i>Figure 15:</i>	External Delivery Function	59
<i>Figure 16:</i>	Integrated Delivery Function with a Non-Distinct Administration Interface	60
<i>Figure 17:</i>	Integrated Delivery Function with a Distinct Administration Interface	60
<i>Figure 18:</i>	Mobile Telephone Systems with Two TSPs	61
<i>Figure 19:</i>	Independently Administered External Pivoted Delivery	62
<i>Figure 20:</i>	Bridged Access	63
<i>Figure 21:</i>	Looped Access	64
<i>Figure 22:</i>	Possible Transmission Schemes for the e-Interface	65
<i>Figure 23:</i>	Possible CDC Protocol Stacks	66
<i>Figure 24:</i>	Possible Circuit-Mode CCC Protocol Stacks	68
<i>Figure 25:</i>	Possible Packet-Mode CCC Protocol Stacks	69
<i>Figure 26:</i>	Dedicated Circuit CCC Delivery	72
<i>Figure 27:</i>	Setup CCC Using Dedicated Circuits	73
<i>Figure 28:</i>	Associate CCC Using Dedicated Circuits	74
<i>Figure 29:</i>	Transfer Call Content Using Dedicated Circuits	75
<i>Figure 30:</i>	Disassociate CCC Using Dedicated Circuits	75
<i>Figure 31:</i>	Dedicated Circuit CCC Release	76
<i>Figure 32:</i>	Trunk Group CCC Delivery	77
<i>Figure 33:</i>	Setup CCCs Using a Trunk from a Trunk Group	78
<i>Figure 34:</i>	Acceptance of CCCs Using a Trunk of a Trunk Group	78
<i>Figure 35:</i>	DF Timed Refusal of a CCC Using a Trunk of a Trunk Group	79
<i>Figure 36:</i>	CF Timed Refusal of a CCC Using a Trunk of a Trunk Group	79
<i>Figure 37:</i>	DF Refusal of a CCC Using a Trunk of a Trunk Group	80
<i>Figure 38:</i>	CF Refusal of a CCC Using a Trunk of a Trunk Group	80
<i>Figure 39:</i>	CCC Continuity Test	81
<i>Figure 40:</i>	Transfer Delayed Call Content Using a Trunk in a Trunk Group	82
<i>Figure 41:</i>	Early Release of CCC Using a Trunk in a Trunk Group	83
<i>Figure 42:</i>	Release CCC Using a Trunk in a Trunk Group	83
<i>Figure 43:</i>	Static Directory Number CCC Delivery	84
<i>Figure 44:</i>	Setup Trunk to Destination	86
<i>Figure 45:</i>	Packet Data CCC Delivery	88
<i>Figure 46:</i>	Separated Content Delivery	90
<i>Figure 47:</i>	Combined Content Delivery	90
<i>Figure 48:</i>	Call Content Distribution	92
<i>Figure 49:</i>	Pivoted Delivery with Distribution	92
<i>Figure 50:</i>	Digit to DTMF Tone Mapping	93

<i>Figure 51:</i>	DTMF C-tone Signaling . . . . .	93
<i>Figure 52:</i>	Dedicated Data Circuit CDC Delivery . . . . .	94
<i>Figure 53:</i>	Dedicated Data Link CDC Delivery . . . . .	95
<i>Figure 54:</i>	Switch Connection Diagram Conventions . . . . .	97

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## Foreword

---

This foreword is not part of this Standard.

The specification of interface compatibility requirements between telecommunication service providers (TSPs) and law enforcement agencies (LEAs) was initiated under the auspices of the ANSI accredited Telecommunications Industry Association Committee TR-45.

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a "safe harbor" under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: "a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106."

There are five annexes in this Standard. All annexes are informative and are not considered part of this Standard.

Standards Proposal Ballot+Clean

Standards Proposal Ballot+Clean

(This page intentionally left blank.)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

File: Front2.fm last modified at July 15, 1997 7:06 PM

# 1 Introduction

## 1.1 General

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a "safe harbor" under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: "a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106."

As used in this Standard, *electronic surveillance* refers to the interception and monitoring of communications (i.e., call content), call-identifying information, or both for a particular telecommunication subscriber as lawfully authorized. In this Standard *intercept subject* or more simply a *subject* is a telecommunication service subscriber whose communications, call-identifying information, or both have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

As a precondition for a TSP's assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve a TSP with the necessary legal authorization identifying the intercept subject, the communications and information to be accessed, and service areas where the communications and information can be accessed. Once this authorization is obtained, the TSP shall perform the access and delivery for transmission to the government's procured equipment, facilities, or services.

LEAs recognize that in many instances the telecommunication services subscribed to by certain intercept subjects may permit a TSP to access and deliver communications and call-identifying information without the TSP having to modify its networks or systems. In these instances, the TSP may be fully compliant with the assistance capability requirements set forth in CALEA. For example, a TSP could effect a central office- or local loop-based interception using conventional methods of access and delivery and fully meet an LEA's electronic surveillance needs.



## 1.2 Purpose

The purpose of this Standard is to facilitate a TSP's compliance with the assistance capability requirements defined in Section 103 of CALEA. This Standard defines services and features to support LAES and the interfaces to deliver intercepted communications and call-identifying information to an LEA when authorized. This Standard also defines a protocol for delivering specific information elements to LEAs. Compliance with this Standard satisfies the "safe harbor" provisions of Section 107 of CALEA and helps ensure efficient and industry-wide implementation of the assistance capability requirements.

## 1.3 Scope

The scope of this Standard is to define the services to support LAES and the interface between a TSP and an LEA.

## 1.4 Organization

Section 2 "References" is a list of references used in the preparation of this Standard.

Section 3 "Definitions and Acronyms" defines words and acronyms that are used in this Standard.

Section 4 "Stage 1 Description: User Perspective" defines the LAES services from the user point of view. The user in this case is the LEA.

Section 5 "Stage 2 Description: Network Perspective" defines the network entities and information flows to implement LAES services from a network point of view.

Section 6 "Stage 3 Description: Implementation Perspective" defines the messages and information elements to implement LAES services from an implementation point of view.

## 2 References

---

### **International Telecommunications Union (ITU) standards:**

---

ITU-T Recommendation G.711, *Pulse code modulation (PCM) of voice frequencies.*

ITU-T Recommendation X.208, *Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).*

ITU-T Recommendation X.209, *Specification of Abstract Syntax Notation One (ASN.1).*

### **American National Standards Institute (ANSI) T1 standards:**

---

ANSI T1.607, *Integrated Services Digital Network (ISDN)—Layer 3 Signaling Specification. for Circuit-Switched Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1).*

### 3 Definitions and Acronyms

**abandoned:** a call attempt that is released by the originating party before it is answered.

**access:** the technical capability to interface with a communications facility, such as a communications line or switch, so that intercepted call-identifying information and call content can be delivered to an LEA.

**AF:** Access Function.

**agent:** a network-based service or device that acts on behalf of a subscriber to send or receive communications (e.g., an interactive screening service, a reminder service, a delayed transmission service).

**AMPS:** Advanced Mobile Phone System, one of several wireless access methods.

**ANSI:** American National Standards Institute.

**answering party:** the party answering a call. This party may be different from the called party (e.g., a called number may alert a number of stations and the answering party may be any one of the alerting stations).

**ASN.1:** Abstract Syntax Notation One.

**associate:** a telecommunication user whose equipment, facilities, or services are communicating with a subject.

**ATM:** Asynchronous Transfer Mode.

**B-channel:** a 56- or 64-kbps ISDN Bearer channel.

**BER:** Basic Encoding Rules.

**BRI:** ISDN Basic Rate Interface consisting of two 64-kbps B-channels and one 16-kbps D-channel.

**CALEA:** Communications Assistance for Law Enforcement Act.

**call:** a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used. A call may have one or more legs.

**call appearance:** an instance of a possible call with direct subscriber control. A party with three call appearances may be involved in and control three calls simultaneously. Some services, such as call forwarding, do not consume call appearances, because the subscriber cannot directly control the call.

**call content** see content.

**call content channel (CCC):** the logical link between the device performing an electronic surveillance access function and the LEA that primarily carries the call content passed between an intercept subject and one or more associates.

**call data channel (CDC):** the logical link between the device performing an electronic surveillance access function and the LEA that prima-

rily carries call-identifying information.

**call deflection:** allows the called party to interactively refuse an incoming call and send that call to another directory number, to voice mail, or to an announcement.

**call delivery** redirects an incoming call to a mobile subscriber.

**call diversion:** is similar to call forwarding, except that the condition may be more complex and dynamic (e.g., its routing decisions may be based upon calling party number, calling party entry of a valid password, time-of-day, day-of-week, day-of-year, calling party location, etc.).

**call forwarding:** is any of several features that redirect a call to another directory number (or voice mail), if a certain condition is met.

**call-identifying information:** defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a [TSP]." As interpreted by this Standard: **destination** is the number of the party to which a call is being made (e.g., called party); **direction** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); **origin** is the number of the party initiating a call (e.g., calling party); and **termination** is the number of the party ultimately receiving a call (e.g., answering party).

**call transfer:** allows a controlling subscriber to connect two other parties and then the controlling subscriber leaves the call.

**called party:** the destination party of a call.

**calling party:** the originating party of a call.

**CCC:** call content channel.

**CCT:** Composite CDMA/TDMA, one of several wireless access methods.

**CDMA:** Code Division Multiple Access, one of several wireless access methods.

**CDC:** call data channel.

**cell:** in a wireless system, the sub-area to which a set of radio resources is allocated.

**CF:** Collection Function.

**channel:** an independent path for communicating between two points.

**CIAP:** Circuit Intercept Access Point.

**circuit:** a switchable bi-directional path between two locations. A circuit may be all or part of a channel. On an end-to-end circuit, separate physical facilities may be used for each segment of the circuit.

**circuit-mode:** a communication using bi-directional paths switched or

connected when the communication is established. The entire communication uses the same path.

**Commission:** defined in CALEA Section 102 (3) to be “the Federal Communication Commission.”

**communication:** in this Standard, communication refers to any wire or electronic communication, as defined in 18 USC 2510.

**communication intercept:** see intercept.

**complete:** a call attempt that is answered.

**connection:** a relationship between two or more parties of a call to allow communication between them.

**content:** defined in 18 USC 2510 (8) to be “when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication.”

**controlling party:** the party invoking a feature.

**CSU:** Channel Service Unit.

**cut-through, full:** completion of a connection in both directions.

**cut-through, partial:** completion of a connection in one direction, usually to allow the calling party to monitor call progress tones from the called end.

**D-channel:** a 16- or 64-kbps ISDN channel carrying control and signaling information and, optionally, packetized information and telemetry.

**DC:** direct current; a signaling method for representing the switchhook state of an instrument to the other end of a call using voltage or current on metallic interfaces or the “A” signaling bit on a DS-0 interface.

**destination:** see call-identifying information.

**DF:** Delivery Function.

**direction:** see call-identifying information.

**disconnect:** a request from one of the parties of the call to release all or part of a connection.

**DSU:** Data Service Unit.

**DTMF:** Dual-Tone Multi-Frequency.

**electronic communications:** defined in 18 USC 2510 (12) to be “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.”

**electronic messaging services:** defined in CALEA Section 102 (4) to be “software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.”

**electronic storage:** defined in 18 USC 2510 (17) to be “(A) any tempo-

rary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

**electronic surveillance:** the statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of call-identifying information. As used in this Standard, *surveillance* refers to a single communication intercept, pen register, or trap and trace. Its usage in this Standard does not include administrative subpoenas for obtaining a subscriber’s toll records and information about a subscriber’s service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

**FG-D: Feature Group D.**

**functional entity:** a system or subsystem capable of providing a defined service. A functional entity may be implemented as a separate physical entity or it may be incorporated with other functional entities in a common physical entity.

**government:** defined in CALEA Section 102 (5) to be “the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.”

**GSM:** Global System for Mobile Communications, one of several wireless access methods.

**handoff:** in a wireless system, the switching of the transmission means used by a call in progress without disruption of this call. Within this Standard handoff is synonymous with handover.

**HDLC:** High-level Data Link Control.

**HLR:** Home Location Register.

**Home Location Register (HLR):** the location register to which a user identity is associated with subscriber information (e.g. equipment identification, directory number, profile information, current Serving System, validation period). The HLR may serve more than one MSC. The HLR may be distributed over more than one physical entity.

**Home System:** the TSP system where a subscriber’s subscription information is retained.

**Hz:** Hertz or cycles per second.

**IAP:** Intercept Access Point.

**IDIAP:** Call-Identifying Information Intercept Access Point.

**idle state:** a state in which there is no active communication path between a subscriber and the network (e.g., while on-hook).

**IN:** intelligent network.

**incomplete:** a call attempt that cannot be routed to its destination (or answered).

**information service:** defined in CALEA Section 102 (6) to be “(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and (B) includes--(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a [TSP’s] internal management, control, or operation of its telecommunication network.” see telecommunication service provider.

**intercept:** defined in 18 USC 2510 (4) to be “the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”

**Intercept Access Point (IAP):** a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject’s equipment, facilities and services are accessed.

**intercept agent:** see agent.

**intercept subject:** a telecommunication service subscriber whose communications, call-identifying information, or both have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

**IP:** Internet Protocol.

**ISDN:** Integrated Services Digital Network.

**ISLP:** Inter-System Link Protocol.

**ISUP:** ISDN User Part.

**ITU-T:** International Telecommunications Union - Telecommunications Standardization Sector (formerly CCITT).

**kbps:** kilobits (1000 bits) per second.

**LAES:** Lawfully Authorized Electronic Surveillance.

**LAESP:** LAES Protocol.

**LAPB:** Link Access Protocol—Balanced.

**LAPD:** Link Access Protocol—D-channel.

**Law Enforcement Agency (LEA):** a government entity with the legal authority to conduct electronic surveillance.

**LEA:** Law Enforcement Agency.

**LEAF:** Law Enforcement Administration Function.

**leg:** a bi-directional call path is associated with each network facility usage attempt and subsequent usage.

**LPP:** Lightweight Presentation Protocol.

**MF:** Multi-Frequency.

**mobile station (MS):** The MS is a telephone set using a radio link with a public or non-public base station to access telephone network services.

**Mobile Switching Center (MSC):** The MSC is an automatic system which constitutes the interface for user traffic between the wireless (cellular or PCS) network and other public switched networks, or other MSCs in the same or other wireless networks.

**MS:** Mobile Station.

**MSC:** Mobile Switching Center.

**MTP:** Message Transfer Part.

**NAMPS:** Narrow AMPS, one of several wireless access methods.

**network address:** an address appropriate to a particular network, e.g., a directory number for the PSTN, an X.121 address for an X.25 network, or an IP address for the Internet.

**off-hook:** the state of a telephone instrument indicating a readiness for service; the DC signaling of the readiness for service state.

**on-hook:** the state of a telephone instrument indicating a request for service disconnect, release, or service idleness; the DC signaling for service disconnect, release, or service idleness.

**origin:** see call-identifying information.

**origination:** an outgoing call attempt.

**packet-mode:** a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network.

**PACS:** Personal Access Communications System, one of several wireless access methods.

**PCM:** pulse code modulation.

**PCS:** Personal Communications Service.

**PCS1900:** one of several GSM-based wireless access methods.

**PDIAP:** Packet Data Intercept Access Point.

**PDU:** Protocol Data Unit.

**pen register:** defined in 18 USC 3127 (3) to be "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of



a wire communication service for cost accounting or other like purposes in the ordinary course of its business.”

**personal mobility:** the ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services according to the user's service profile. Personal mobility involves the network capability to locate the terminal associated with the user for the purposes of addressing, routing, and charging of the user's calls.

**POTS:** Plain Old Telephone Service. This usually refers to loop start lines with DTMF (tone) dialing or decadic (rotary) dialing.

**PPP:** Point-to-Point Protocol.

**PRI:** ISDN Primary Rate Interface consisting of twenty-three 64-kbps B-channels and one 64-kbps D-channel.

**PSTN:** Public Switched Telephone Network.

**pulse code modulation (PCM):** a method for communicating audio information using a 56 or 64 kbps digital bit stream. In the United States most PCM is encoded using the  $\mu$ law rules.

**Redirecting System:** the TSP system where incoming calls bound to a subscriber arrive for redirection instruction. This is called an Originating System in *IS-41*, although the calls may be originated on another system.

**recall:** a previously answered call or call attempt that alerts the controlling party.

**registration:** in wireless systems, the process that informs the Home System of the location and presence of a mobile station.

**release:** to place facilities used for a connection in the idle state where they can be used for other connections.

**roaming:** in a wireless system, the movement of a mobile station within or between wireless service areas where the mobile station can be located and can receive service.

**Serving System:** the TSP system currently providing telecommunication service to a subscriber, especially a roaming mobile subscriber.

**short message service (SMS):** a packet-mode data service, intended for transmission of small data messages, for wireless subscribers.

**SLIP:** Serial Link Internet Protocol.

**SMS:** short message service.

**SPAF:** Service Provider Administration Function.

**SSIAP:** Serving System Identification Intercept Access Point.

**subject:** see intercept subject.

**surveillance:** within this Standard surveillance refers to electronic surveillance; see electronic surveillance.